

Securing Communications with a DNS-based PKI

Paco Hope
Applications Development Manager



213 East Water Street, Suite 1
(804) 245-5300

paco@tovaris.com
<http://www.tovaris.com/>

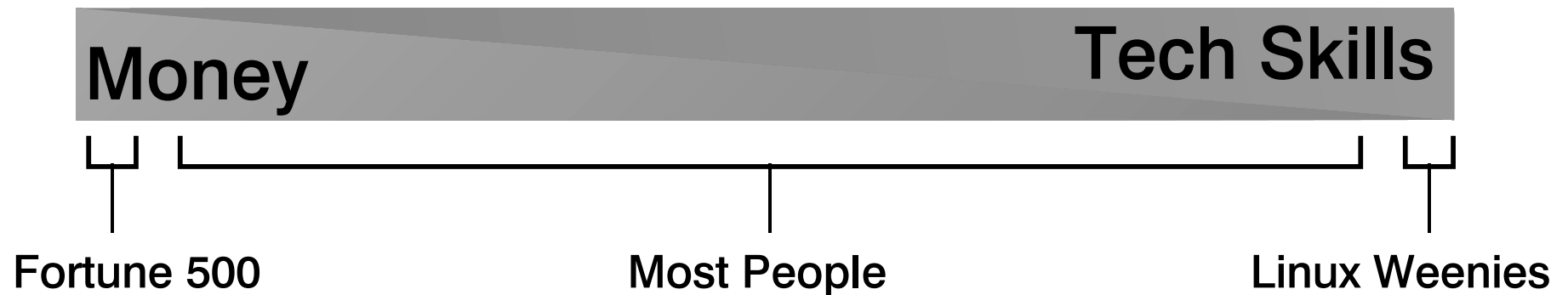
Agenda

- ◆ Our description of the problem
- ◆ Our goals
- ◆ Our products
 - Mithril Secure Server™ (Server-based email encryption)
 - SecureTier™ (DNS-based certificate delivery)
- ◆ Comparisons
 - Performance
 - Scalability
 - Ease of use

Problem Space

Cryptography only practical for small minority

- ◆ Enterprises
 - Lots of money and time
- ◆ Technophiles
 - Skills to use free tools



Problem Space

“Castle” Approach Overlooks Interoperability

- ◆ Firewalls \approx Moats
- ◆ Cannot encrypt if you cannot find and use certificates

Available crypto +
certificate discovery

widespread adoption



The Goal

Cryptography All the Time

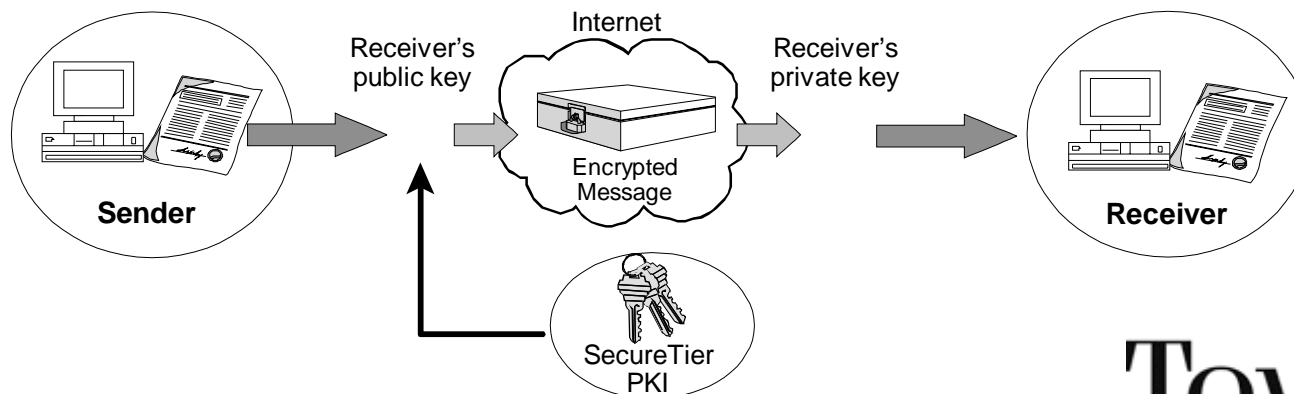
- ◆ Every participant in every transaction
 - E-mail
 - E-commerce
 - Secure web
 - Etc
- ◆ Digital Identity Management
 - Certificate distribution is important first step
 - Making it usable everywhere



Mithril Secure Server™

Overview

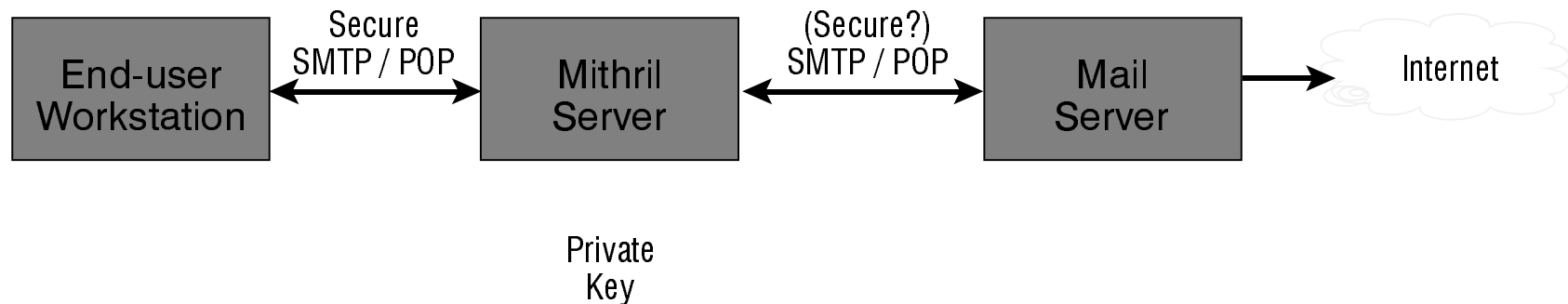
- ▶ Secure e-mail by default whenever possible
- ▶ Simple integration into existing e-mail infrastructure
- ▶ Easy adoption by end-users (no software)
- ▶ Deliver secure messages to non-Mithril users
- ▶ Scalable
- ▶ Compatible with existing solutions (X.509, S/MIME)



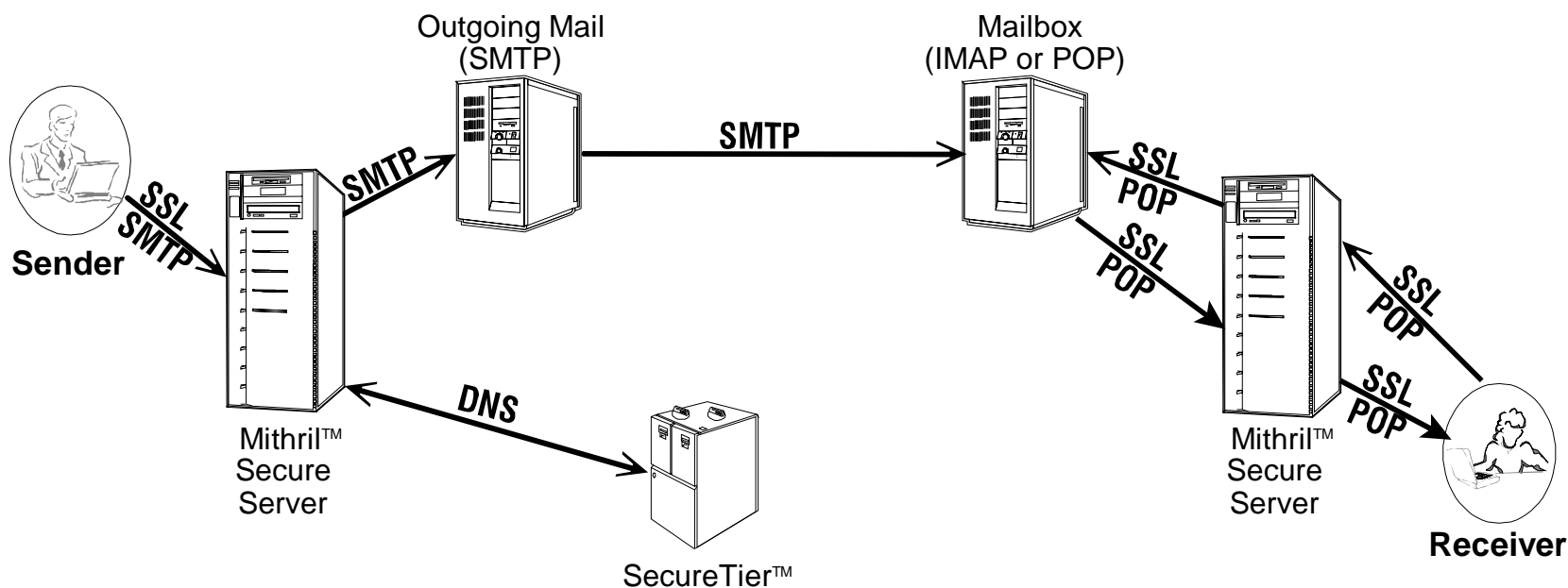
Mithril: E-Mail Proxy

Standards-Compliant Component Architecture

- ◆ Mail Protocols
 - SMTP (Sending Mail)
 - IMAP (Reading Mail)
 - POP (Reading Mail)
- ◆ Cryptography Engine
 - X.509, S/MIME (OpenSSL)
- ◆ Connection to PKI
 - DNS-based SecureTier



Sending a Message with Mithril



- ◆ Decrypt Private Key
- ◆ Discover Recipient Certificate
- ◆ Encrypt Outbound Mail

- ◆ Decrypt Private Key
- ◆ Decrypt Inbound Message

Mithril in a Nutshell

CA and Certificate Management for e-mail

- ◆ Issues end-user certificates
- ◆ Maintains key pairs for users
- ◆ Performs key lookups for participants
- ◆ Encrypts and decrypts automatically
- ◆ Uses SecureTier

What is SecureTier™?

- ◆ Certificate lookup and delivery mechanism
- ◆ Based on DNS
- ◆ Queries based on e-mail address
- ◆ Returns authoritative answers quickly

Domain Name Service

“It’s not just for host names any more”

- ◆ Host Lookups

- `www.tovarish.com` ⇒ `209.145.64.15`

- ◆ IP address lookups

- `209.145.64.15` ⇒ `www.tovarish.com`

- ◆ Mail server lookups

- Tovarish.com mail serviced by `mail.tovarish.com`

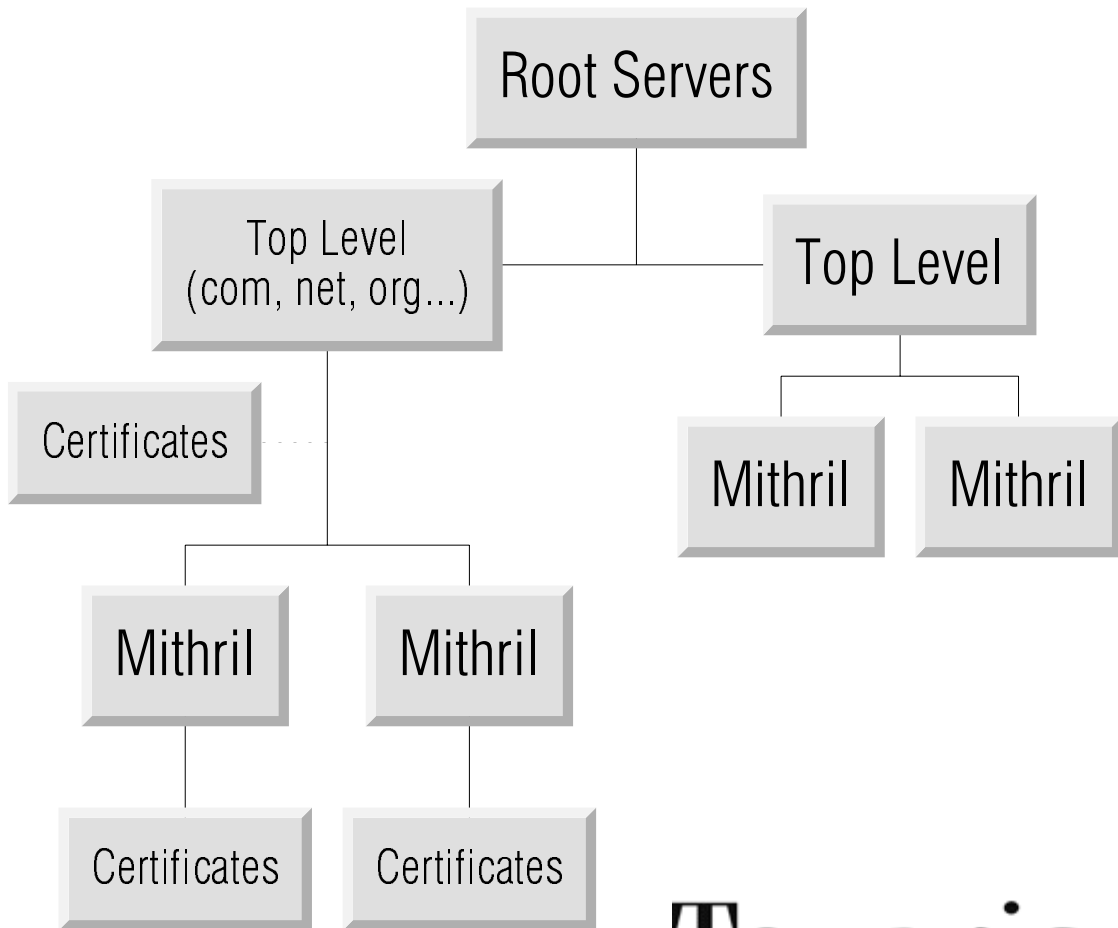
- ◆ Tovarish adds:

- `paco@tovarish.com` ⇒ [public key certificate]

SecureTier™ Overview

DNS-style Hierarchy

- ◆ Hierarchical
- ◆ Redundant
- ◆ Scalable
- ◆ Geographically distributed
- ◆ Partitioned Authority



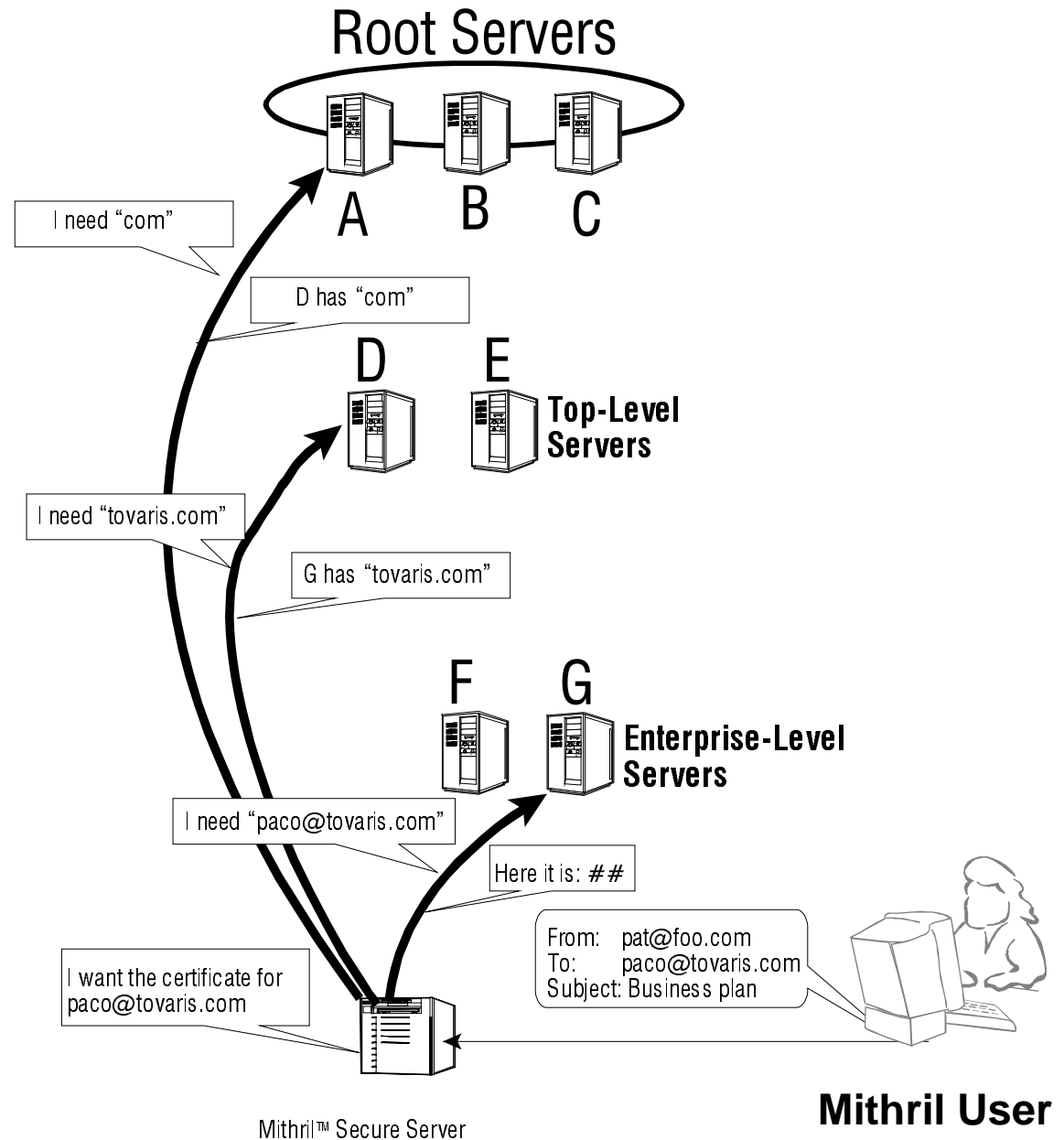
Operations

Some nitty gritty

- ◆ All SecureTier nodes are BIND version 9 from ISC
- ◆ Certificates stored in standard CERT records
- ◆ Independent of regular DNS
- ◆ Tovarish operates roots and top-level servers
- ◆ Same name registry

Anatomy of a DNS Lookup

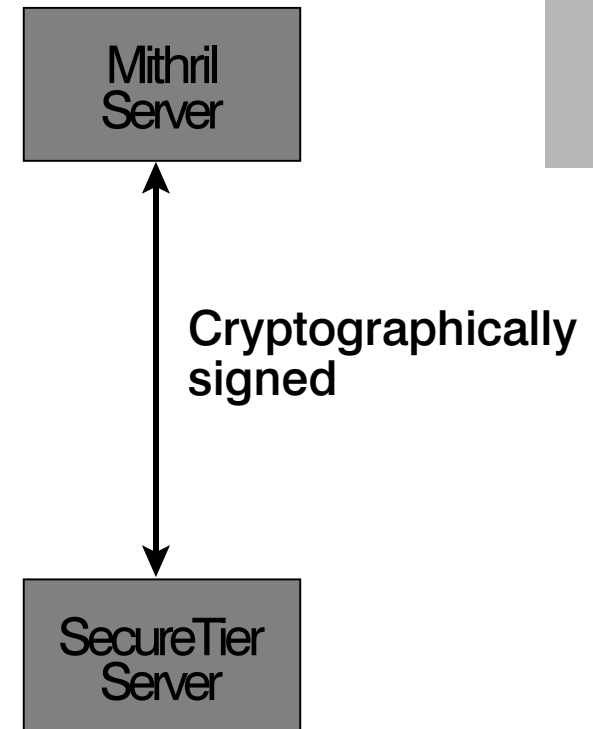
Starting with an email address and finding a certificate



SecureTier Operations

Safety of a PKI

- ◆ Updates use TSIG
 - MD5 signatures
 - Access restricted by keys
- ◆ Timestamp and hash
 - Prevents spoofing, injection of bad data
 - Prevents replay of negative answers (DoS)
- ◆ Not signing DNS zones
 - CERTs already signed
 - Unnecessary overhead



Compare Efficiency

DNS

- ✓ Handful of UDP packets (yes and no)
- ✓ Aggressive caching throughout hierarchy
- ✓ Simple query syntax

LDAP

- ✗ Unbounded number of TCP queries (yes and no)
- ✗ No caching by default, except maybe ad hoc
- ✗ Complex query syntax (servers and clients more complicated)

Compare Scalability

DNS

- ✓ Dynamically discover authorities
- ✓ Partition easily by domain components
- ✓ Can easily add intermediate caching or redundant servers (discovered dynamically)

LDAP

- ✗ Difficult to discover authorities
- ✗ Can partition, but must have some master server
- ✗ Redundancy is harder

Compare Ease of Use

DNS

- ✓ Clients make one query
- ✓ Universal OS support

LDAP

- ✗ Clients make many queries
- ✗ Patchwork OS support

Interesting DNS Issues

It's not as easy as it looks

- ◆ X.509 arbitrary strings
 - ▶ Non-hierarchical
 - ▶ Hard to store/lookup
- ◆ Firewalls interfere with UDP
- ◆ LDAP ↔ DNS gateway
 - ▶ Search
 - ▶ Publish
- ◆ Kitchen sink not included

Putting it All Together

Mithril + SecureTier = DNS-based PKI

- ◆ Mithril

- ▶ Certificate creation, maintenance
- ▶ Encryption, decryption
- ▶ Certificate lookups

- ◆ SecureTier

- ▶ Mapping e-mail addresses to certificates
- ▶ Scaling to the size of the Internet
- ▶ Fastest thing out there



Thank You

Questions? Comments?

Points of Contact



James J. Snare
Director, Strategic
Development
Tovarís, Inc.

(703) 622-0772
(804) 245-5300 x311

jsnare@tovaris.com

Paco Hope
Applications Development
Manager
Tovarís, Inc.

(804) 245- 5300 x118

paco@tovaris.com

<http://www.tovarís.com/>